Involutionをもつガロア拡大 (ガロア理論について)

AUTHOR(S):

神崎, 熙夫

数理解析研究所講究録
235巻 1975年 44-65

involution をもつガロア拡大

阪市大　神崎熙夫

1. Rosenberg-Wareの定理の拡張

一般に単位元をもつ非可換環を考える。Aをinvolution $A \to A$; $a \rightsquigarrow \bar{a}$, ($\overline{ab} = \bar{b}\bar{a}$, $\overline{a+b} = \bar{a} + \bar{b}$, $\bar{\bar{a}} = a$, $a, b \in A$) をもつ環とする。有限生成射影的A-左加群 M 及び写像 g : $M \times M \to A$ が $\overline{g(x,y)} = g(y,x)$, $g(ax+by, z) = ag(x,z) + bg(y,z)$, ($x, y \in M$, $a, b \in A$) をみたすとき、$g = (M, g)$ をエルミットA-左加群とよぶ。特に写像 $M \to \mathrm{Hom}_A(M, A)$: $x \rightsquigarrow g(-,x)$ が1対1写像をなすとき、g は非退化であると云う。環$A \supset B$ が次の条件をみたすとき、involution をもつG-ガロア拡大とよぶ。即ち、1) $A \supset B$ はG-ガロア拡大、即ちGは環Aの有限個の自己同型写像からなる群で $A^G = B$ をみたし、$\sum_i x_i y_i = 1$ 、$\sum_i x_i \sigma(y_i) = 0$ ($\sigma \neq I \in G$) を満たすAの元$x_1 \cdots x_n$, $y_1, \cdots, y_n$ (G-ガロアシステムとよぶ) が存在。 2) Aは $\overline{\sigma(a)} = \sigma(\bar{a})$, ${}^\forall \sigma \in G$, $a \in A$, を満たすinvolutionをもつ。

$A \supset B$ がinvolutionをもつG-ガロア拡大ならばAは次の

様にエルミットB-左加群と見られる。CをAの中心とし、$C_0 = \{c\in C ; \bar{c}=c\}$の単元の全体$U_C(A)$に対し、$t_G^u(a)=\sum_{\sigma\in G}\sigma(ua)$ $u\in U_C(A)$, $a\in A$, $t_G^1=t_G$ とおく。任意の$u\in U_C(A)$に対し、$b_t^u : A\times A\to B$ を $b_t^u(x,y)=t_G^u(x\bar{y})$ と定義するとき、$b_t^u=(A, b_t^u)$は非退化エルミットB-左加群をなす（非退化であることは、$u\bar{y}=\sum_i x_i t_G^u(y_i\bar{y})=\sum_i x_i b_t^u(y_i,y)$ $({}^\forall y\in A)$, 及び、$f\in \mathrm{Hom}_B(A,B)$ は $f(x)=t_G^u(u^{-1}x\sum_i x_i f(y_i))=b_t^u(x,\overline{\sum_i x_i f(y_i)})$ と表わされることよりうる。但し $x_1,\cdots x_n$, $y_1,\cdots,y_n$ はAのG-ガロアシステムである）。involutionをもつG-ガロア拡大に於て、involutionが特に恒等写像の場合、環は必然的に可換環となり普通の意味のG-ガロア拡大になる。この場合自明なinvolutionをもつG-ガロア拡大とよぶ事とする。

エルミットB-左加群(U, g)に対し、$U^*=\mathrm{Hom}_B(U,B)$を、$(bf)(x)=f(x)\bar{b}$, $(b\in B,\ f\in U^*,\ x\in U)$ によってB-左加群と見て、直和$U\oplus U^*$を作り、$h_g : (U\oplus U^*)\times(U\oplus U^*)\to B$; $(x+f,\ x'+f')\leadsto \overline{f(x')}+f'(x)+g(x,x')$ によって定義されたエルミットB-左加群$(U\oplus U^*, h_g)$を考える。この様な$(U\oplus U^*, h_g)$にisometricなエルミットB-左加群をmetabolic B-左加群とよぶ（エルミットB-左加群(M,g), (M',g')に於て $g'(\varphi(m),\varphi(n))=g(m,n)$ $(m,n\in M)$ を満たすB-同型写像$\varphi : M\to M'$ をisometryとよび、(M,g)と(M',g')はisometric

であると云う)。又 $I: B\times B \to B ; (x,y) \rightsquigarrow x\bar{y}$ によって定義されたエルミット B-左加群 (B, I) を $\langle 1\rangle_B$ で表わす。

定義 involution をもつ G-ガロア拡大 $A\supset B$ が次の条件を満たす $U_c(A)$ の元 u をもつとき、$A\supset B$ は奇数型であると云う。即ち、(A, b_t^u) は、或る metabolic B-左加群 (N, h_m) と $\langle 1\rangle_B$ の直交和に isometric である:$(A, b_t^u) \cong \langle 1\rangle_B \perp (N, h_m)$。

Scharlau の定理([5] p.195, Th. 1.6)より体の場合に次の定理を得る。

定理1. 体 K, L に対し、$L\supset K$ を involution をもつ G-ガロア拡大とする。$L\supset K$ が奇数型である為の必要十分条件は $[L:K]=$ 奇数である。

証明、$L\supset K$ が奇数型ならば、明らかに $[L:K]=$ 奇数。逆に $[L:K]=2m+1$ とする。先ず、$L\supset K$ が自明な involution をもつ G-ガロア拡大である場合を考える。適当な $a\in K$ に対して、$L=K[a]=K\oplus Ka\oplus\cdots\oplus Ka^{2m}$. $f: L\to K$ を、$f(1)=1$, $f(a^i)=0$, $i=1,2,\cdots,2m$ で定義された K-1次写像とする。(L, b_t^1) の非退化性から、$b_t^1(x,u)=f(x)$ $(x\in L)$ を満たす L の元 $u\neq 0$ が存在する。$b_t^u(x,y)=f(xy)$, $(x,y\in L)$, $(L, b_t^u)= K\perp (Ka\oplus\cdots\oplus Ka^{2m})$, $(K, b_t^u)=\langle 1\rangle_K$ である。$(Ka\oplus\cdots\oplus Ka^{2m})$ は次に示す補題1を用いて metabolic B-左加群となることが得られる。次に $L\supset K$ を自明でない involution をもつ G-ガロ

ア拡大とする。$L_0=\{x\in L\ ;\ \bar{x}=x\}$, $K_0=L_0\cap K$と置く。このとき、$[L:K]=$奇数より$[L:L_0]=[K:K_0]=2$を得る。よって、$L=K\cdot L_0\cong K\otimes_{K_0}L_0$, $L_0\supset K_0$は自明なinvolutionをもつG-ガロア拡大、従って、前述の場合より$U_c(L)=\{c\in L_0 : c\neq 0\}$の元$u$が存在し、$(L_0, b_t^u)\cong\langle 1\rangle_{K_0}\perp(N,h)$, (N,h)は或るmetabolic K_0-左加群となる。従って、$(L, b_t^u)\cong(K\otimes_{K_0}L_0, b_t^u)\cong\langle 1\rangle_K\perp(K\otimes_{K_0}N, h')$となり、$(K\otimes_{K_0}N, h')$は又metabolic K-左加群、故に$L\supset K$は奇数型である。

補題1. Bをinvolutionをもつ環、(M, q)を非退化エルミットB-左加群とする。(M, q)がmetabolic B-左加群である為の必要十分条件は、$N=N^{\perp}$を満たすMの直和因子Nが存在することである(但し$N^{\perp}=\{x\in M;\ q(x,y)=0\ {}^{\forall}y\in N\}$).

証明　(M, q)がmetabolicならば、$(M, q)\cong(U\oplus U^*, h_q)$、$(U^*)^{\perp}=U^*$、従って$U^*$に同型な$M$の直和因子$N$で$N^{\perp}=N$を満たすものがある。逆に$q=(M,q)$が$M=N\oplus N'$, $N^{\perp}=N$を満たすB-部分加群Nをもつとする。写像$N\to(N')^*=\mathrm{Hom}_B(N', B)$; $x\rightsquigarrow q(-,x)$はB-同型写像となり、$(N'\oplus N'^*, h_q)$は写像$M=N\oplus N'\longrightarrow(N')^*\oplus N'$; $x+x'\rightsquigarrow q(-,x)+x'$により$(M, q)$にisometricになる。故に$(M, q)$はmetabolic B-左加群である。

標数$\neq 2$の体K及びその拡大体Lについて次の結果が知られている。I. Springerの定理([8]又は[5] P.198参照) $[L:K]$

＝奇数のとき、体K上の2次形式qがL上でisotropicならばqはK上でisotropicである。即ち体K上の2次形式から作られるWitt ring $W(K)$から体L上のWitt ring $W(L)$への係数拡大で生ずる写像$W(K)\to W(L)$が単写である。II. Rosenberg－Wareの定理（[6]又は[5] P. 214参照）．L⊃Kを奇数位数のガロア群Gをもつガロア拡大とする。Gの元σ、L上の2次形式$q=\langle a_1, a_2, \cdots, a_n\rangle$ $(a_i\in L)$に対し、$\sigma(q)=\langle\sigma(a_1), \sigma(a_2), \cdots, \sigma(a_n)\rangle$によってW(L)にGの元の作用を定義するとき，W(L)はG-ringをなす．$W(L)^G=\{[q]\in W(L) : \sigma([q])=[q], {}^\forall\sigma\in G\}$はW(L)の部分環で、係数拡大により生ずる準同型写像$W(K)\to W(L)$は$W(K)$から$W(L)^G$への同型写像を与える．この定理は[7]に於て可換半局所環にまで拡張されている。こゝではこの定理をより一般な環に於けるinvolutionをもつ奇数型G-ガロア拡大に拡張する。

再びA⊃Bをinvolutionをもつ G-ガロア拡大とする。A上の（又はB上の）非退化エルミット左加群とisometryとから成るカテゴリーは直交和⊥を演算に持ち、metabolic左加群からなる部分カテゴリーをもつ。良く知られる様にWitt-Grthendieck群WG(A)（又はWG(B)），Witt群W(A)（又はW(B)）を構成することが出来る。今$q=(M, q)$をエルミットA-左加群とする。$\sigma\in G$に対し、$\sigma^*(q)$を次の様に定義する。

$\sigma^*(g)=({}_\sigma M,\sigma g)$, ${}_\sigma M$ は加群としてはMと等しく、Aの元 a の作用を $a\cdot m=\sigma^{-1}(a)m$ によって定義したA-左加群を意味し、σg は、$\sigma g: {}_\sigma M\times{}_\sigma M\to A$; $(x,y)\longmapsto\sigma(g(x,y))$ を表わす。$\sigma^*(g)$ はエルミットA-左加群となる。g が非退化ならば $\sigma^*(g)$ も非退化である。写像 $t_G: A\to B$ に対し、エルミットA-左加群 $g=(M, g)$ からエルミットB-左加群 $t_{G*}(g)=({}_BM, t_Gg)$ が $t_Gg(x,y)=t_G(g(x,y))$, $x,y\in M$ によって定義され、g が非退化ならば $t_{G*}(g)$ も非退化となる。エルミットB-左加群 $h=(N,h)$ に対し、写像 $i: B\hookrightarrow A$ によって、エルミットA-左加群 $i^*(h)=(A\otimes_B N, ih)$ が $ih:(A\otimes_B N)\times(A\otimes_B N)\longrightarrow A$; $(a\otimes x, a'\otimes x')\longmapsto a h(x,x')\overline{a'}$ で定義される。h が非退化ならば $i^*(h)$ も非退化となる。σ^* $(\sigma\in G)$, t_{G^*} i^* はmetabolic左加群をmetabolic左加群に移すからWitt群の準同型写像 $\sigma^*: W(A)\to W(A)$, $t_{G^*}: W(A)\to W(B)$, $i^*: W(B)\to W(A)$ をひき起こす事は、容易に知られる。$G^*=\{\sigma^*: W(A)\to W(A) ; \sigma\in G\}$, $W(A)^{G^*}=\{[g]\in W(A) ; \sigma^*([g])=[g] ; {}^\forall\sigma^*\in G^*\}$ と置く。$T_{G^*}=\sum_{\sigma\in G}\sigma^*$ は $W(A)$ から $W(A)^{G^*}$ の中への準同型写像を与える。次の定理が得られる。

定理2. Bを可換環、Aを(一般に非可換)B-多元環とする。A⊃Bがinvolutionをもつ奇数型G-ガロア拡大ならば、

1) $i^*: W(B)\to W(A)$ は単写、$i^*(W(B))=T_{G^*}(W(A))$ であり従って、$W(B)\cong T_{G^*}(W(A))$ である。

2). $t_{G^*}: W(A) \to W(B)$ は全字かつ分解、$\mathrm{Ker}\, t_{G^*} = \mathrm{Ker}\, T_{G^*}$.
従って、$W(A) \cong T_{G^*}(W(A)) \oplus \mathrm{Ker}\, T_{G^*} = i^*(W(B)) \oplus \mathrm{Ker}\, t_{G^*}$.

3) もし A が可換環ならば、$T_{G^*}(W(A)) = W(A)^{G^*}$、従って $i^*: W(B) \longrightarrow W(A)^{G^*}$ は同型字像である。

この定理と前定理とより、次の結果が得られる。

系1. L, K を体、$L \supset K$ を involution をもつ G-ガロア拡大とする。もし $|G| = [L:K] =$ 奇数ならば、$i^*: W(K) \to T_{G^*}(W(L)) = W(L)^{G^*}$ は同型字像、かつ $t_{G^*}: W(A) \to W(B)$ は全字かつ分解、従って、$W(L) \cong W(A)^{G^*} \oplus \mathrm{Ker}\, t_{G^*}$ である。

以下この節では定理2の証明を行なう。その為に、

定理3. $A \supset B$ を involution をもつ G-ガロア拡大とする。$W(A)$ 上で等式 $i^* \circ t_{G^*} = T_{G^*}$ が成り立つ。

証明　$g = (M, g)$ を非退化エルミット A-左加群とする。A の G-ガロアシステム $x_1, \cdots, x_n, y_1, \cdots, y_n$, 及び各 $\sigma \in G$ に対し、A-準同型字像 $e_\sigma: A \otimes_B M \to A \otimes_B M$; $a \otimes m \longmapsto \sum_i a\sigma(x_i) \otimes y_i m$ が定義される事は、等式 $e_\sigma(ac \otimes m) = e_\sigma(a \otimes \sigma^{-1}(c) m)$, $(\forall c \in A)$ が成立する事より知られる。簡単な計算から、$e_\sigma \circ e_\sigma = e_\sigma$,

$e_\sigma \circ e_\tau = 0$ $(\sigma \neq \tau)$, $\sum_{\sigma \in G} e_\sigma = I$ が示される。従って $A \otimes_B M = \sum_{\sigma \in G} \oplus e_\sigma(A \otimes_B M)$. 　字像 $\zeta_\sigma: {}_\sigma M \to e_\sigma(A \otimes_B M)$; $m \leadsto e_\sigma(1 \otimes m)$ は A-同型字像をなし、$A \otimes_B M$ は $\sum_{\sigma \in G} \oplus {}_\sigma M$ に A-同型になる。一方 $i^* \circ t_{G^*}(g) = (A \otimes_B M, i t_G g)$ に於て、次の等式が得られる。

$$i t_G q(e_\sigma(1\otimes m),\ e_\sigma(1\otimes n)) = \sigma(q(m,n)),$$
$$i t_G q(e_\sigma(1\otimes m),\ e_\tau(1\otimes n)) = 0 \quad (\sigma \neq \tau).$$

これは $i^* t_{G^*}(q) = (A\otimes_B M,\ i t_G q) = \sum_{\sigma\in G} \perp e_\sigma(A\otimes_B M)$. 又、$\zeta_\sigma$ は $\sigma^*(q) = ({}_\sigma M, \sigma q)$ から $i^* t_{G^*}(q)$ の部分空間 $e_\sigma(A\otimes_B M)$ への isometry を与える事を意味する。従って $i^* t_{G^*}(q) \cong \sum_{\sigma\in G} \perp \sigma^*(q)$ を得る。

定理4. B を可換環、A を B-多元環、$A \supset B$ は involution をもつ奇数型 G-ガロア拡大とする。u を $(A, b_t^u) \cong \langle 1\rangle_B \perp h_m$ (h_m : metabolic) を満たす $\amalg_c(A)$ の元とするとき、$W(B)$ 上で等式 $t_{G^*}^u \circ i^* = I$, エルミット A-左加群としての isometry $\sum_{\sigma\in G} \perp \sigma^*(\langle u\rangle) \cong \langle 1\rangle_A \perp i^*(h_m)$ が成立する。但し $\langle u\rangle$ は、$A\times A \to A : (x, y) \longmapsto u x \bar{y}$ によって定義されたエルミット A-左加群を表わす.

証明 $q = (M, q)$ を非退化エルミット B-左加群とする. エルミット B-左加群として $t_{G^*}^u \circ i^*(q) = (A\otimes_B M,\ t_G^u i q) \cong (A, b_t^u) \otimes (M, q)$ が成立する事が, $t_G^u i q(a\otimes m, a'\otimes m') = t_G(u a q(m,m')\bar{a'}) = t_G(u a \bar{a'}) q(m,m') = b_t^u(a,a')\cdot q(m,m')$ より知られる。よって、B が可換環である事に注意して、$t_{G^*}^u \circ i^*(q) \cong (\langle 1\rangle_B \perp h_m)\otimes q \cong q \perp h_m\otimes q$、$h_m\otimes q$ は又 metabolic B-左加群となり、$t_{G^*}^u \circ i^* = I$ が得られる. (A, b_t^u) の定義より、$b_t^u \cong t_{G^*}(\langle u\rangle)$ が知られる. 従って、定理3から

$i^*\circ t_{G^*}(\langle u\rangle) \cong \sum_{\sigma\in G}\perp \sigma^*(\langle u\rangle)$, $\sum_{\sigma\in G}\perp \sigma^*(\langle u\rangle) \cong i^*\circ t_{G^*}(\langle u\rangle) \cong i^*(b_t^u)$
$= i^*(\langle 1\rangle_B \perp h_m) = \langle 1\rangle_A \perp i^*(h_m)$ を得る。

定理2の証明. $U_c(A)$の任意の元uに対し、エルミットA-左加群$g=(M,g)$のuによるscaling $^ug=(M,{}^ug)$を$^ug: M\times M\to A$; $(x,y)\mapsto ug(x,y)$により定義する。uによるscalingは$W(A)$の自己同型写像をひき起こす。今uを定理4に於ける様に取る。uによるscalingでひき起こされる自己同型写像 $\mu: W(A)\to W(A)$ に対し、$t_{G^*}^u = t_{G^*}\circ\mu$。定理4より、$t_{G^*}^u\circ i^* = I$、従って、$t_{G^*}\circ\mu\circ i^* = I$。故に$i^*: W(B)\to W(A)$は単写、$t_{G^*}: W(A)\to W(B)$は全写かつ分解する。定理3より、$i^*\circ t_{G^*} = T_{G^*}$、従って、$i^* = T_{G^*}\circ\mu\circ i^*$ 故に $\mathrm{Im}\, i^* = \mathrm{Im}\, T_{G^*}$, $\mathrm{Ker}\, t_{G^*} = \mathrm{Ker}\, T_{G^*}$ となり、$i^*: W(B)\to T_{G^*}(W(A))$ は同型写像、$W(A)=\mu\circ i^*(W(B))\oplus \mathrm{Ker}\, t_{G^*} \cong i^*(W(B))\oplus \mathrm{Ker}\, t_{G^*}$.
もしAが可換環ならば、$W(A)$は$\perp$及び$\otimes$によって導入された加法と乗法に関し可換環をなし単位元$[\langle 1\rangle_A]$をもつ。$W(A)^{G^*}$はその部分環をなし、$T_{G^*}(W(A))$は$W(A)^{G^*}$のイデアルをなす。定理4より、$[\langle 1\rangle_A]\in T_{G^*}(W(A))$、従って$T_{G^*}(W(A)) = W(A)^{G^*}$を得る。故に$i^*: W(B)\to W(A)^{G^*}$は同型写像である。

2. 半局所環に於けるinvolutionをもつ奇数型ガロア拡大.

A, Bを可換環、A⊃Bはinvolutionをもつ G-ガロア拡大とする。A⊃Bが奇数型ならば容易に$|G|$=奇数が示される（$|M|$

は集合Mの元の個数を表わす)。今次の命題を考える。

(命題0) involutionをもつG-ガロア拡大が奇数型である為の必要十分条件は$|G|=$奇数である。

定理5. A,Bを可換半局所環、$A\supset B$はinvolutionをもつG-ガロア拡大とする.次の各場合には(命題0)は真である。

(場合I) involutionは自明で、Bの各極大イデアル$\mathfrak{m}$に対し$|B/\mathfrak{m}|\geqq|G|$であるとき、

(場合II) involutionは自明でなく、Bの各極大イデアル$\mathfrak{m}$に対し、次の2条件が満たされるとき.: 1) $|B/\mathfrak{m}|\geqq|G|^2$, 2) もし$\overline{\mathfrak{m}}=\mathfrak{m}$ならば、Aのinvolutionは$A/\mathfrak{m}A$の自明でないinvolutionをひき起こす.

(場合III) Bは極大イデアル$\mathfrak{m}$をもつ局所環で、Aのinvolutionは自明でなく、$A/\mathfrak{m}A$上に自明なinvolutionをひき起こし、$|B/\mathfrak{m}|\geqq|G|$、かつ$B/\mathfrak{m}$は標数$\neq 2$の体か又は有限体であるとき。

以下この節ではこの定理の証明を行なう.

補題2. A,Bを半局所環、$A\supset B$は自明なinvolutionをもつG-ガロア拡大とする。もしBの各極大イデアル$\mathfrak{m}$に対し、$|B/\mathfrak{m}|\geqq|G|$ならば、次の事柄が成り立つ.

1) $A=B[a]=B\oplus Ba\oplus\cdots\oplus Ba^{n-1}$ $(n=|G|)$かつ$\{a^i : 0\leqq i<n\}$はAのB-基底となるAの元aが存在し、aの$B[X]$に属する最小多項式$F(X)=X^n+d_1X^{n-1}+\cdots+d_n$に於て、$d_n$はBで可逆的。

2) $h(1)=1$, $h(a^i)=0$, $i=1,2,\cdots,n-1$, によって定義された B-1次写像 $h: A\to B$ に対し、$h(x)=t_G(ux)=b_t'(u,x)$ $(\forall x\in A)$ を満たす A の可逆元 u が存在する.

証明、始め、B は体であると仮定する. A のすべての原始巾等元を $e_1, e_2, \cdots, e_m$ とするとき、 $A=Ae_1\oplus\cdots\oplus Ae_m$ は Be_i のガロア拡大体 Ae_i $(i=1,2,\cdots,m)$ の直和である. $G_1=\{\sigma\in G;\sigma(e_1)=e_1\}$、$\sigma_i(e_1)=e_i$ $(i=1,2,\cdots,m)$ と置く. $|G|=m|G_1|$. $Ae_1\supset Be_1$ は G_1-ガロア拡大であり、$\sigma_i: Ae_1\to Ae_i$ は B-多元環として同型写像である. $B[X]$ の分離的既約多項式 $f(X)$ が存在して. $Ae_i\cong B[X]/(f(X))$, $i=1,2,\cdots,m$. B の元 $b_1=0$, $b_2,\cdots,b_m$ を適当に選らんで $f(X+b_1), f(X+b_2),\cdots, f(X+b_m)$ が互に異なる多項式になる様に取る事が出来る. B の代数的閉体に於ける $f(X)=0$ のすべての根を $\alpha_1,\alpha_2,\cdots,\alpha_\ell$ $(\ell=|G_1|)$ とする. もし $b_1=0, b_2,\cdots, b_r$ $(1\leq r<m)$ を、$f(X+b_1), f(X+b_2),\cdots, f(X+b_r)$ が互に相異なる多項式となる様に B から選らべたとする. $|B|\geqq|G|=m\ell>r\ell$ より、$\alpha_1-b_{r+1}\neq\alpha_i-b_j$, $i=1,2,\cdots,\ell$, $j=1,2,\cdots r$, を満たす B の元 b_{r+1} を選らぶ事が出来る. よって帰納的に $b_1,b_2,\cdots,b_m$ を選らぶ事が出来る. $F(X)=f(X+b_1)f(X+b_2)\cdots f(X+b_m)$ と置く. 従って、

$$B[X]/(F(X))\cong B[X]/(f(X+b_1))\oplus\cdots\oplus B[X]/(f(X+b_m))\cong Ae_1\oplus\cdots\oplus Ae_m$$

$=A$. よって、$A=B[a]=B\oplus Ba\oplus\cdots\oplus Ba^{n-1}$ となる $a\in A$ が存在し、a の $B[X]$ に於ける最小多項式は $F(X)=X^n+d_1X^{n-1}+\cdots+d_n$

となる．$f(X+b_i)$ は既約であるから $d_n \neq 0$ である．$h : A \to B$ を $h(1)=1$, $h(a^i)=0$, $i=1,2,\cdots,n-1$ によって定義された B-1次写像とする．(A, b_t^1) の非退化性より、$h(x)=b_t^1(x,u)=t_G(xu)$ $(^\forall x\in A)$ を満たす $u\in A$ が存在する．u は A の可逆元である事を示す．$\mathfrak{n}=\{x\in A ; xu=0\}$ と置く．$h(x)=t_G(xu)$ $(x\in A)$ より $\mathfrak{n}\subset \mathrm{Ker}\, h = Ba\oplus\cdots\oplus Ba^{n-1}$ を得る．任意の $x\in\mathfrak{n}$ に対し、$x=b_1'a+b_2'a^2+\cdots+b_{n-1}'a^{n-1}$ と表わされる．$(a^{n-1}+d_1a^{n-2}+\cdots+d_{n-1})x$ $=(a^n+d_1a^{n-1}+\cdots+d_{n-1}a)(b_1'+b_2'a+\cdots+b_{n-1}'a^{n-2})=-d_n(b_1'+b_2'a+\cdots+b_{n-1}'a^{n-2})\in\mathfrak{n}\subset Ba\oplus\cdots\oplus Ba^{n-1}$．故に $d_nb_1'=0$ 従って $b_1'=0$, $b_2'a+\cdots+b_{n-1}'a^{n-2}\in\mathfrak{n}$．再びこれを繰り返して、$b_1'=b_2'=\cdots=b_{n-1}'=0$ 即ち $x=0$ を得る．よって $\mathfrak{n}=0$．A は Artin 環であるから、u は可逆的である．次に B を一般の半局所環とする．B の Jacobson 根基 J に対し、剰余環 B/J のすべての原始巾等元を $e_1, e_2, \cdots, e_t$ とする．$A/JA\, e_i \supset B/J\, e_i$ $(i=1,2,\cdots,t)$ 及び $A/JA=\sum_{i=1}^{t}\oplus A/JA\, e_i\supset\sum_{i=1}^{t}\oplus B/J\, e_i$ は共に G-ガロア拡大である．$B/J\, e_i$ は体であり、前述より $A/JA\, e_i=B/J\, e_i[\alpha_i]$ $=B/J\, e_i\oplus B/J\, e_i\alpha_i\oplus\cdots\oplus B/J\, e_i\alpha_i^{n-1}$ を満たす $A/JA\, e_i$ の元 α_i が存在する $(i=1,\cdots,t)$．$\alpha=\alpha_1+\alpha_2+\cdots+\alpha_t$ と置くと、$A/JA=B/J\oplus B/J\,\alpha\oplus\cdots\oplus B/J\,\alpha^{n-1}$ であり、$\{1,\alpha,\alpha^2,\cdots,\alpha^{n-1}\}$ は A/JA の B/J-基底をなす．A に於ける α の代表元 a を取れば、中山の補題により、$A=B\oplus Ba\oplus\cdots\oplus Ba^{n-1}$ となり、$\{1,a,\cdots,a^{n-1}\}$ は A の B-

基底をなす．又 a の $B[X]$ に於ける最小多項式を $F(X)=X^n+d_1X^{n-1}+\cdots+d_n$ と置けば、d_n は前半より J を法として可逆的であり、従って、d_n はBに於て可逆的である．$h(1)=1$, $h(a^i)=0$ $i=1, 2, \cdots, n-1$, により定義された B-1次写像 $h: A\to B$ に対し、$b_t^1(x,u)=t_G(ux)=h(x)$ $(x\in A)$ を満たす A の元 u が存在する．前半より u は JA を法として可逆的であるから、A で又可逆的である．

(場合I) に於ける定理5の証明．A, B を半局所環、$A\supset B$ を自明な involution をもつ G-ガロア拡大とし、$|G|=$奇数、Bの各極大イデアル $\mathfrak{m}$ に対し、$|B/\mathfrak{m}|\geq|G|$ と仮定する．補題2より、$A=B\oplus Ba\oplus\cdots\oplus Ba^{n-1}$, $\{1, a, \cdots, a^{n-1}\}$ は A の B-基底となる $a\in A$ が存在し、$h(1)=1$, $h(a^i)=0$ $(1\leq i\leq n-1)$ により定義された B-1次写像 $h: A\to B$ に対し、$h(x)=t_G(ux)=b_t^u(1,x)$ $(x\in A)$ を満たす A の可逆元 u が存在する．よって $(A, b_t^u)=B\perp(Ba\oplus\cdots\oplus Ba^{n-1})$ は非退化であり、従って $(Ba\oplus Ba^2\oplus\cdots\oplus Ba^{n-1})$ も非退化となる．$Ba\oplus Ba^2\oplus\cdots\oplus Ba^{n-1}$ が metabolic B-左加群であることを示す為に $r=\frac{n-1}{2}$, $N=Ba\oplus\cdots\oplus Ba^r$ と置く．補題1より $N^\perp\subset N$ を示せば十分である．その為には $N^\perp\cap(Ba^{r+1}\oplus\cdots\oplus Ba^{n-1})=0$ が示されゝば良い．今 $N^\perp\cap(Ba^{r+1}\oplus\cdots\oplus Ba^{n-1})$ の元 $c=b_1a^{r+1}+\cdots+b_ra^{n-1}\neq0$ が存在すると仮定する．$b_1=b_2=\cdots=b_{k-1}=0$, $b_k\neq0$ となる k がある．$F(X)=X^n+d_1X^{n-1}$

$+\cdots+d_n$ を a の $B[X]$ に於ける最小多項式、$L(X)=-(X^{n-r-k}+d_1X^{n-r-k-1}+\cdots+d_{r-k}X)$, $H(X)=d_{r-k+1}X^{r+k}+\cdots+d_n$ と置く。このとき、$F(X)=-L(X)X^{r+k}+H(X)$, $L(a)a^{r+k}=H(a)$ であり、$L(a)=-(d_{r-1}a+\cdots+d_1a^{n-r-k-1}+a^{n-r-k})\in N$ である。$c\in N^{\perp}$ より

$$
\begin{aligned}
0=b_t^u(c,\ L(a))&=h(c\cdot L(a))\\
&=h((b_k+b_{k+1}a+\cdots+b_r a^{n-r-k-1})\ a^{r+k}L(a))\\
&=h((b_k+b_{k+1}a+\cdots+b_r a^{n-r-k-1})H(a))\\
&=h((b_k+b_{k+1}a+\cdots+b_r a^{n-1-r-k})(d_{r-k-1}a^{r+k}+\cdots+d_n))\\
&=b_kd_n.
\end{aligned}
$$

よって、$b_k=0$ となり仮定に反する。即ち $Ba\oplus\cdots\oplus Ba^{n-1}$ は metabolic B-部分加群で、$(A,\ b_t^u)=\langle 1\rangle_B\perp(Ba\oplus\cdots\oplus Ba^{n-1})$, $A\supset B$ は奇数型である。

補題3. A, B を半局所環、$A\supset B$ は自明でない involution をもつ G-ガロア拡大、$|G|=$奇数 と仮定する。このとき A の involution は B の上に自明でない involution をひき起こす。

証明 $A_0=\{a\in A\ ;\ \overline{a}=a\}$ と置く。A の involution が B の上で自明であると仮定すれば、$A_0\supset B$ である。A の involution 及び A の恒等写像からなる群を H で表わすとき、$A_0=A^H$ である。$A\supset A_0$ は H-ガロア拡大である事が次の様に示される。$e_1, e_2, \cdots, e_m$ を A のすべての原始巾等元、$\overline{e_{2i-1}}=e_{2i}$, $i=1,2,\cdots r$, $\overline{e_j}=e_j$, $j=2r+1,\cdots,m$ とする。$e_i'=e_{2i-1}+e_{2i}$ $(i=1,2,\cdots r)$, e_j $(j=2r+1,\cdots,m)$ は A_0 に属する互に直交する巾等元で、

$1=\sum_{i=1}^{r} e_i' + \sum_{j=1}^{m} e_j$ を満たす。Ae_j は $0, e_j$ 以外に巾等元をもたず $Ae_j \supset A_0 e_j$ は分離的、$(Ae_j)^H = A_0 e_j$ であるから、$Ae_j \supset A_0 e_j$ ($j=2r+1,\cdots,m$) はH-ガロア拡大となる。一方 Ae_i' ($i=1,2,\cdots,r$) について、$Ae_i' = A_0 e_{2i-1} + A_0 e_{2i}$ を満たす。何故ならば任意の $a \in Ae_i'$ に対し、$a_0 = a e_{2i-1} + \bar{a} e_{2i}$, $a_0' = \bar{a} e_{2i-1} + a e_{2i}$ は $A_0 = A^H$ に属し、$a = a e_{2i-1} + a e_{2i} = a_0 e_{2i-1} + a_0' e_{2i} \in A_0 e_{2i-1} \oplus A_0 e_{2i}$ を得る。従って、$Ae_i' = A_0 e_{2i-1} \oplus A_0 e_{2i} \supset A_0 e_i'$ は自明なH-ガロア拡大であり、$A = \sum_{i=1}^{r} \oplus Ae_i' \oplus \sum_{j=1}^{m} \oplus Ae_j \supset A_0 = \sum \oplus A_0 e_i' \oplus \sum \oplus A_0 e_j$ はH-ガロア拡大となる。故に $|G| = [A:B] = [A:A_0][A_0:B] = 2\cdot[A_0:B]$. これは仮定に反する。よってB上に自明でない involution をひき起こす。

(場合II) に於ける定理5の証明. A, B を半局所環、$A \supset B$ を自明でない involution をもつG-ガロア拡大、$|G|=$ 奇数、B の各極大イデアル $\mathfrak{m}$ に対し $|B/\mathfrak{m}| \geq |G|^2$、$\bar{\mathfrak{m}} = \mathfrak{m}$ ならば A の involution は $A/\mathfrak{m}A$ 上自明でない involution をひき起こすと仮定する。$A_0 = \{a \in A; \bar{a} = a\}$, $B_0 = A_0 \cap B$, H を involution と恒等写像とからなる群とする. $B \supset B_0$ について、B の極大イデアル $\mathfrak{m}$ に対し、もし $\bar{\mathfrak{m}} \neq \mathfrak{m}$ ならば $b - \bar{b} \notin \mathfrak{m}$ を満たす $b \in B$ が、又 $\bar{\mathfrak{m}} = \mathfrak{m}$ ならば仮定より又その様な b が存在するから、[2], Th. 1.3 より $B \supset B_0$ はH-ガロア拡大となることが得られる。今 $x_1, x_2, \cdots, x_n$, $y_1, \cdots, y_n$ を B の H-ガロアシステムとする

ときAの任意の元aは、$a=\sum_i t_H(ax_i)y_i$と表わされる．従って、$A_0\otimes_{B_0}B\to A$；$a_0\otimes b\rightsquigarrow a_0b$は全字、$\sum a_i\otimes b_i\in A_0\otimes_{B_0}B$に対し、$\sum a_ib_i=0$ならば、$\sum_i a_i\otimes b_i=\sum a_i\otimes t_H(b_ix_j)y_j=\sum t_H(a_ib_ix_j)\otimes y_j=0$ よって、$A_0\otimes_{B_0}B\cong A$を得る。B_0も又半局所環になるから、BはB₀-基底$\{1, v\}$をもち、これはAのA₀-基底でもある．$A_0\supset B_0$がG-ガロア拡大となることは次の様に見られる．明らかに$A_0^G=B_0$、A_0の極大イデアル$\mathfrak{p}_0$に対し、$\mathfrak{p}\supset A\mathfrak{p}_0$なるAの極大イデアル$\mathfrak{p}$を取る事が出来る．$A\supset B$はG-ガロア拡大であるから、各$\sigma(\neq I)\in G$に対し、$a-\sigma(a)\notin\mathfrak{p}$をみたす$a\in A$が存在し、$a=a_0+a_1v$，$a_0, a_1\in A_0$と表わされる．従って、$a-\sigma(a)=(a_0-\sigma(a_0))+(a_1-\sigma(a_1))v\notin\mathfrak{p}$であり、$a_0-\sigma(a_0)\notin\mathfrak{p}_0$．又は$a_1-\sigma(a_1)\notin\mathfrak{p}_0$を得る．[2], Th.1.3 より$A_0\supset B_0$はG-ガロア拡大となる．$B_0$の任意の極大イデアル$\mathfrak{m}_0$に対し、$\mathfrak{m}\cap A_0=\mathfrak{m}_0$を満たすAの極大イデアル$\mathfrak{m}$を取れば、$[B/\mathfrak{m}:B_0/\mathfrak{m}_0]\leqq 2$，$|B_0/\mathfrak{m}_0|\geqq\sqrt{|B/\mathfrak{m}|}\geqq|G|$を得る．自明なinvolutionをもつG-ガロア拡大$A_0\supset B_0$に（場合I）を適用して、$A_0\supset B_0$は奇数型になる．従って、次の補題を用いれば、$A\supset B$が奇数型である事を得る．

補題4．A, Bを可換環、$A\supset B$は自明でないinvolutionをもつG-ガロア拡大とする．$A_0=\{a\in A;\ \bar{a}=a\}$，$B_0=A_0\cap B$と置く．もし$A_0\supset B_0$がG-ガロア拡大ならば$A\cong A_0\otimes_{B_0}B$であ

り、$A_0 \supset B_0$ が奇数型ならば、$A \supset B$ も奇数型である。

証明. $x_1, \cdots, x_n$, $y_1, \cdots, y_n$ を A_0 の G-ガロアシステムとするとき、$A_0 \otimes_{B_0} B \to A$; $a_0 \otimes b \mapsto a_0 b$ が同型写像であることは、$a \in A$ に対し、$a = \sum x_i t_G(y_i a) \in A_0 B$, $\sum a_i b_i = 0$ $(a_i \in A_0, b_i \in B)$ ならば $\sum a_i \otimes b_i = \sum x_j t_G(y_j a_i) \otimes b_i = \sum x_j \otimes t_G(y_j a_i) b_i = \sum x_j \otimes t_G(y_j a_i b_i) = 0$ より得る. もし $A_0 \supset B_0$ が奇数型ならば、A_0 の可逆元 u と、metabolic B_0-加群 h_m が存在して、$(A_0, b_t^u) \cong \langle 1 \rangle_{B_0} \perp h_m$ となる. $i : B_0 \hookrightarrow B$ に対し、$i^*(b_t^u) = (B \otimes_{B_0} A_0, i b_t^u) \cong (A, b_t^u) \cong \langle 1 \rangle_B \perp i^*(h_m)$, $i^*(h_m)$ は又 metabolic B-加群になるから、$A \supset B$ は奇数型である。

(場合Ⅲ) に於ける定理5の証明. B を極大イデアル m をもつ局所環、$A \supset B$ は自明でない involution をもつ G-ガロア拡大、A/mA 上に自明な involution をひき起こすとする。更に $|G| =$ 奇数、$|B/m| \geqq |G|$ で、B/m は標数 $\neq 2$ の体か又は有限体と仮定する. 補題2より $A = B \oplus Ba \oplus \cdots \oplus Ba^{n-1}$, $\{1, a, \cdots, a^{n-1}\}$ は A の B-基底、となる $a \in A$ が存在する. もし B/m が標数 $\neq 2$ の体ならば、2 は B で可逆的、a の代りに $\frac{a+\bar{a}}{2} = a'$ を取る事が出来、$a' \equiv a \pmod{mA}$, $\overline{a'} = a'$ を満たす. もし B/m が標数 2 の有限体ならば、A/mA は標数 2 の有限体の直和であり、$A/mA \to A/mA$; $[x] \mapsto [x^2]$ は自己同型写像となり、$c^2 \equiv a \pmod{mA}$ を満たす $c \in A$ を選ぶ事が出来る. a の代りに $a' = c \cdot \bar{c}$ を取

るならば、$a' \equiv a \pmod{\mathfrak{m}A}$，$\overline{a'} = a'$ が満たされる．以上の理由から、$A = B \oplus Ba' \oplus \cdots \oplus Ba'^{n-1}$，$\{1, a', \cdots, a'^{n-1}\}$ は A の B-基底、$\overline{a'} = a'$ となる A の元 a' を選らぶ事が出来る．従って、B-1次写像 $h : A \to B$; $h(1) = 0$，$h(a'^i) = 0$，$i = 1, \cdots, n-1$，は $\overline{h(x)} = h(\overline{x})$ $({}^\forall x \in A)$ を満たし、$h(x) = b'_t(x, u) = t_G(x\overline{u})$ $(x \in A)$ により定まる A の可逆元 u は、$b'_t(x, u) = h(x) = \overline{h(\overline{x})} = \overline{t_G(\overline{x}\overline{u})} = t_G(xu) = b'_t(x, \overline{u})$，$({}^\forall x \in A)$ を満たす．従って、$\overline{u} = u$ であり、$u \in U_c(A)$ を得る．(場合 I) に於ける証明と全く同様にして、(A, b''_t) は $\langle 1 \rangle_B$ と metabolic B-左加群の直交和に isometric になり、$A \supset B$ は奇数型となる．

3．involution をもつ G-ガロア拡大の例

例1．可換環 B 上の非退化 quadratic B-加群 (V, q) を考える．(V, q) は直交基底 $v_1, v_2, \cdots v_n$ をもつと仮定する．即ち、$(V, q) = Bv_1 \perp \cdots \perp Bv_n$，従って、2 及び $q(v_i)$ は B で可逆的である．ρ_{v_i} を $\rho_{v_i}(x) = x - \dfrac{B_q(x, v_i)}{q(v_i)} v_i$，$(x \in V)$ によって定義された symmetry とする $(i = 1, 2, \cdots, n)$．(V, q) の Clifford 多元環を $C(V, q) = C_0(V, q) \oplus C_1(V, q)$ とする．$C(V, q)$ は $\mathbb{Z}/(2)$-次数加群であり $C_0(V, q)$ は 0 次の同次部分、$C_1(V, q)$ は 1 次の同次部分を表わす．ρ_{v_i} は $C(V, q)$ の多元環-自己同型写像 $\hat{\rho}_i$ に拡張される．$C(V, q)$ は $\overline{x_1 x_2 \cdots x_r} = x_r x_{r-1} \cdots x_2 x_1$ $(x_i \in V)$ によって定義された involution をもち、$\hat{\rho}_i(\overline{y}) = \overline{\hat{\rho}_i(y)}$，$y \in C(V, q)$ を満たす．G

を $\hat{\rho}_1, \hat{\rho}_2, \cdots, \hat{\rho}_n$ で生成された $C(V,q)$ の自己同型写像からなる群とし、$A=C(V,q)$ と置く。

定理6. $A=C(V,q), B, G$ を上述のようにする。このとき、$A\supset B$ は、involution をもつ G-ガロア拡大となり、$G\cong(\hat{\rho}_1)\times\cdots\times(\hat{\rho}_n)$ である。

証明. $(V,q)=Bv_1\perp Bv_2\perp\cdots\perp Bv_n$ に対し、$A=C(V,q)\supset B$ が G-ガロア拡大であること、及び $G\cong(\hat{\rho}_1)\times\cdots\times(\hat{\rho}_n)$ であることは n に関する帰納法で示される。$n=1$ に対して、$C(Bv_1,q)\cong B[X]/(X^2-q(v_1))$ は B の分離的2次拡大であり、$C(Bv_1,q)^{(\hat{\rho}_1)}=B$ により、$C(Bv_1,q)\supset B$ は、$(\hat{\rho}_1)$-ガロア拡大となる。$V_{n-1}=Bv_1\perp\cdots\perp Bv_{n-1}$ に対し、$C(V_{n-1},q)\supset B$ は G_{n-1}-ガロア拡大、$G_{n-1}\cong(\hat{\rho}_1)\times\cdots\times(\hat{\rho}_{n-1})$ と仮定する。$V=V_{n-1}\perp Bv_n$ より、$C(V,q)\cong C(V_{n-1},q)\hat{\otimes}_B C(Bv_n,q)$ となり、仮定より、$C(V_{n-1},q)$ の G_{n-1}-ガロアシステム $x_1,x_2,\cdots x_s, y_1,y_2,\cdots,y_s$ 及び $C(Bv_n,q)$ の $(\hat{\rho}_n)$-ガロアシステム $u_1,u_2,\cdots,u_t, w_1,w_2,\cdots,w_t$ が存在する。このとき、x_i,y_i,u_j,w_j は同次部分から取ることが出来る。$\{(-1)^{\partial y_i\partial u_j}x_i\otimes u_j,\ y_i\otimes w_j\ ;\ 1\leqq i\leqq s,\ 1\leqq j\leqq t\}$ は $C(V,q)=C(V_{n-1},q)\hat{\otimes}C(Bv_n,q)$ の $G=G_{n-1}\otimes(\hat{\rho}_n)$-ガロアシステムとなる。又 $C(V,q)^G=C(V_{n-1},q)^{G_{n-1}}\otimes C(Bv_n,q)^{(\hat{\rho}_n)}=B$ より、$C(V,q)\supset B$ は G-ガロア拡大、$G\cong(\hat{\rho}_1)\times\cdots\times(\hat{\rho}_n)$ を得る。先に述べた事より、$A\supset B$ は involution をもつ G-ガロア拡大である事

が知られる。

例2. $A \supset B$ を involution をもつ G-ガロア拡大とする。A 上の n 次の完全行列環を A_n で表わし、G の元は成分に作用させる事により、A_n の自己同型写像に拡張され、その群を再び G で表わす事とする。$A_n \to A_n$; $(a_{ij}) \longmapsto {}^t(\overline{a_{ij}})$ によって A の involution は A_n の involution に拡張される（${}^t(\overline{a_{ij}})$ は (a_{ij}) の転置行列を表わす）。このとき、$A_n \supset B_n$ は又 involution をもつ G-ガロア拡大となる。$A \supset B$ が奇数型ならば、$A_n \supset B_n$ も又奇数型になる事が次のように示される。もし $u \in U_c(A)$ に対し $(A, b_t^u) \cong \langle 1 \rangle_B \perp h_m$, ($h_m$: metabolic B-左加群）ならば $u \in U_c(A) \subset U_c(A_n)$ であり、$(A_n, b_t^u) = (B_n \otimes_B A, \ i b_t^u) \cong \langle 1 \rangle_{B_n} \perp i^*(h_m)$, $i^*(h_m)$ は又 metabolic B_n-左加群となる。但し、$i : B \hookrightarrow B_n$. よって、$A_n \supset B_n$ は又奇数型である。

例3. $A \supset B$ を involution をもつ G-ガロア拡大とする。自明な因子団をもつ接合積 $\Delta(A,G) = \sum_{\sigma \in G} \oplus A u_\sigma$ を考え、u_1 はその単位元と仮定する事が出来る。M を忠実な $\Delta(A,G)$-左加群で $[u_\sigma(m), u_\sigma(n)] = \sigma([m,n])$, $(m, n \in M, \sigma \in G)$ を満たす非退化エルミット形式 $[\ ,\ ] : M \times M \to A$ をもつと仮定する。$M^G = \{m \in M ; u_\sigma m = m, \ {}^\forall \sigma \in G\}$ は B-左部分加群をなし、$[\ ,\ ] \,|\, M^G \times M^G$ は、M^G から B への非退化エルミット形式をひき起こす。更に $M = AM^G \cong A \otimes_B M^G$ が満たされる。もし M^G が有限生成射影的 B-加群

かつ．B-generator ならば、$\Lambda = \mathrm{Hom}_A(M,M)$, $\Gamma = \mathrm{Hom}_{\Delta(A,G)}(M,M)$ について、(Λ及びΓの元はMの元に右側から作用させる事とする)，$[m, n\lambda] = [m\bar{\lambda}, n]$ $(\forall m, n \in M, \lambda \in \Lambda)$ によって与えられる involution $\Lambda \to \Lambda : \lambda \mapsto \bar{\lambda}$ をもち、Gの元σに対し、

$m\sigma'(\lambda) = u_\sigma((u_\sigma^{-1}m)\lambda)$ $(m \in M, \lambda \in \Lambda)$ によって定義される自己同型写像$\sigma' : \Lambda \to \Lambda$が定まり、かゝる$\sigma'$の全体$G'$に対して、$\Lambda \supset \Gamma$は involution をもつ$G'$-ガロア拡大となる．このとき、$G \to G'$; $\sigma \mapsto \sigma'$ は同型写像である．(証明は[3]を参照)

以上に於て述べたエルミット加群についての基本概念は[1]による。内容は、[3]，[4]の解説である．

参考文献

[1] H.Bass : Unitary K-theory, Springer lecture notes 343 (1973).

[2] S.U.Chase, D.K.Harrison and A.Rosenberg : Galois theory and Galois cohomology of commutative rings, Mem. Amer. MAth. Soc. No. 52 (1965).

[3] T.Kanzaki : On Galois extension with involution of rings,

[4] T.Kanzaki and K.Kitamura : On odd type Galois extension with involution of semi-local rings, Proc. Japan Acad. 51 (1975) 117-122.

[5] T.Y.Lam : The algebraic theory of quadratic forms, Benjamin (1973).

[6] A.Rosenberg and R.Ware : The zero-dimensional Galois cohomology of Witt ring, Invension math. 11 (1970), 65-72.

[7] M.Knebusch, A.Rosenberg and R.Ware : Signatures on semi-local rings, J.

Algebra 26 (1973), 208-250.

[8] T.A.Springer : Sur les formes d'indices zero, C. R. Acad. Sci. 234 (1952) 1517-1519.